SECTION 2
IMPLEMENTATION OVERVIEW

2.1 DESCRIPTION. Sites for installation of DSRS-related COTS software will be approved and scheduled through the SRP. It is assumed that installation of the COTS software will be conducted in conjunction with installation of the DSRS.

The implementation procedures for the DSRS and its related COTS support software include: configuring the hardware and each of the individual COTS software products in accordance with vendor-supplied procedures; determining the site-specific system environment variables to be used; creating the necessary accounts and directory structures; and then performing the installation as documented in Section 4 or 5 of this document, as it corresponds to your UNIX operating system.

2.2 CONTACT POINT. Contact the SRP with questions relating to implementation of DSRS and its related COTS software. Problems encountered will be coordinated with the SRP.

2.3 SUPPORT MATERIALS. The following documents will be provided with the DSRS hardware/software system:

a. *System Administration Manual (AM) for the DSRS*

b. *Librarian Manual (LM) for the DSRS*

c. *DSRS for Windows User Manual (WUM)*

d. *DSRS for X/Motif User Manual (XUM)*

Refer to Section 3 of this document for pre-installation requirements.

2.4 TRAINING. Contact the SRP for information about available DSRS and related COTS support software installation training.

2.5 PERSONNEL ORIENTATION. Sites can make arrangements with the SRP representatives for instruction and guidance to help site personnel adapt to the new system.

2.6 PERSONNEL REQUIREMENTS. It is the responsibility of the implementing site to arrange for personnel to install the DSRS and related COTS software.

a. Personnel designated by the SRP will have the following responsibilities:

(1) Act as the functional proponent for DSRS,
(2) Provide the DSRS to sites,
(3) Provide implementation policy,
(4) Provide technical support,
(5) Accept and respond to problem reports and enhancement requests, and

(6) Provide User documents.

b. Operation of the system requires designation of skilled personnel at the site where the system resides, with the following responsibilities:

(1) Install the DSRS-related COTS software,
(2) Install the DSRS software,
(3) Exercise the system to ensure it has been properly installed, and
(4) Provide Supervisor/Librarian to administrator of the DSRS.

The DSRS manuals outline specific reponsibilities and duties for the System Administrator, Supervisor, and Librarian. (Other specific changes to the operations of the SRP and the remote sites will be identified and addressed by the SRP, as appropriate.)

2.7 TASKS. Table 2-I lists each task required for installation and a description of the task. SRP personnel will perform all software installation activities at a central location.

Table 2-I. Installation Tasks

Task	Description
Configure Hardware	Each system must conform to the minimum hardware requirements addressed in paragraph 3.3a of this document.
Install COTS Support Software	The required COTS support software listed in Table 3-I.
Provide Support Documentation	It is recommended that each site have the documents specified in each section. Additionally, all User and Installation documentation should be available for each DSRS-related COTS software package to be installed.
Determine Environment Variables	The following environment variables will need to be determined before the installation is begun: ● tape device available; ● the unique ORACLE SID for the DSRS database; ● the account to be used for the DSRS installation; ● the passwords for the root and ORACLE accounts; ● the directory structure where the DSRS will be installed; and ● the directory structure where the ORACLE database files will be installed.
Create User Accounts and Directories	The accounts and directories will be created as desired and required.
Unload DSRS Tape	The DSRS tape will be unloaded into the directory.

Task	Description
Modify Files	The necessary file modifications will be made specific to the installation.
Run **dsrs_install**	The script file, **dsrs_install**, will be executed to create the database and install the database information into the database.
Run Test Condition Requirements	The TCRs will be performed and verified to assure that the COTS software performs as required.
Run System Tests	The system tests will be performed and verified for quality assurance. The system tests will take approximately two days to perform.
Transfer DSRS V6.0 Database Info	The DSRS 6.0 database can be updated into the DSRS database using the script file, **update60to605**.
Transfer DSRS V5.2 Database Info	The DSRS 5.2 database can be updated into the DSRS database using the script file, **update52to605**.

2.8 SECURITY. Because the DSRS contains sensitive unclassified information that must maintain high levels of confidentiality, integrity and availability, an appropriate level of security must be exercised in the installation of the COTS software that is to support the DSRS environment. Additionally, adequate security precautions must be taken to protect the hardware platforms upon which the DSRS is to reside.

2.8.1 Data Protection Objectives. The DSRS and its associated COTS support software require protection in order to:

a. Maintain a high level of confidentiality to prevent unauthorized access to proprietary information;

b. Prevent the misuse of Government computer resources;

c. Protect the reusable assets from unauthorized modification which could cause harm to the DSRS or, more importantly, user sytems; and

d. Ensure the availability of information to meet customer requirements.

2.8.2 Minimum Required Security Classification. The *National Policy on Controlled Access Protection* (NTISSP) No. 200, 15 July 1987, established the policy for automated information systems (AISs) that are accessed by multiple users with different authorizations to the information contained in the system (i.e., System High security mode). The policy mandated that these systems provide automated controlled access protection and that this minimal level of protection be provided within five years of the policy's issuance. The Department of Defense carried the policy forward in

Directive 5200.28 which specified requirements for AISs that handle classified, sensitive unclassified, or unclassified information. "For AISs that process or handle classified and/or sensitive unclassified information, and that, based upon the prescribed risk-assessment procedure, require at least controlled access protection, the Directive mandates an implementation timetable of 1992."

Controlled access protection policies are based upon a fundamental assumption that the AIS processing environment is one of mutually trusting and cooperating users. Recognition of this fact is critical to understanding the objectives of controlled access protection. The features, assurances, and, most importantly, the underlying system architecture of an AIS that provides controlled access protection are not and do not purport to prevent malicious or concerted actions aimed at circumventing the protection provided. Controlled access protection provides:

a. Protection and control over who can logon to the system;

b. Mechanisms that will enable the AIS to make decisions regarding access to resources based upon the expressed wishes of its users (with no assurance that concerted, malicious actions cannot circumvent this mechanism); and

c. The capability to generate a reliable log of user actions and to guarantee its correctness.

Based on these mandates, the DSRS has the minimum required security classification of C2 which was determined by performing the Risk Assessment prescribed in Enclosure 4, DoD Directive 5200.28. It was also determined by this risk assessment that the DSRS operates in the *System High security mode* which means that all users have the appropriate clearances or authorization; however, *all users do not have the same need-to-know for all information* stored on the system.

All COTS software packages will be considered UNCLASSIFIED and deemed to be stand-alone and error-free at the time of receipt. Once integrated into the DSRS system, COTS software will be subject to the same security requirements as the DSRS software.

2.8.3 Security Implementation Procedures. Specific security implementation procedures for DSRS are contained in the *DSRS Trusted Facility Manual*. The *DSRS Trusted Facility Manual* is directed towards the administrators of the DSRS (and its related COTS software) and provides specific details on how to:

a. Configure and install the DSRS and its related COTS support software packages according to the requirements dictated by controlled access protection (i.e., C2 security classification);

b. Operate the DSRS according to controlled access protection guidelines;

c. Control functions and privileges; and

d. As applicable, generate, examine, and maintain audit files, as well as the detailed audit record structure, for each type of audit record structure.